AO 106 (Rev. 06/09) Application for a Search Warrant

FILED

DEC 17 2021

Mark C. McCartt, Clerk
U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
information associated with fendawilson@gmail.com stored at premises owned, maintained, controlled, or operated by Google LLC

Case No. 21-MJ-890-SH

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2119(1)	**Carjacking**
18 U.S.C. §§ 924(c)(1)(A)(ii)	**Carrying, Using, and Brandishing a Firearm During and in Relation to a Crime of Violence**
18 U.S.C. §§ 922(g)(1) and 924(a)(2)	**Felon in Possession of a Firearm and Ammunition**
18 U.S.C. §§ 922(a)(6) and 924(a)(2)	**False Statement to Acquire a Firearm**
18 U.S.C. § 371	**Conspiracy**

The application is based on these facts:

See Affidavit of Bryant Ward, attached hereto.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Bryant L. Ward
Applicant's signature

TFO Bryant Ward, FBI
Printed name and title

Sworn to before me and signed by telephone.

Date: 12/17/21

Judge's signature

City and state: Tulsa, OK

Susan E. Huntsman, U.S. Magistrate Judge

Printed name and title

Affidavit in Support of an Application for a Search Warrant

I, Bryant Ward, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Police Officer with the Tulsa Police Department and have been since 2015. I am currently assigned as a Robbery Detective. I am also a cross-commissioned Creek Lighthorse and Cherokee Marshal. I also hold a Special Law Enforcement Commission with the Bureau of Indian Affairs and am a sworn FBI Task Force Officer. I am an investigative or law enforcement officer within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make

arrests for, offenses enumerated in Title 18, United States Code, Section 2516. As part of my duties as Robbery Detective, I investigate violent crimes such as carjacking and robberies, including those involving the use or threatened use of a firearm.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, reviews of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Since this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

4. Based on Affiant's training, experience, and the facts as set forth in this affidavit, there is probable cause to believe the identified Google Account contains evidence and instrumentalities of violations of 18 U.S.C. § 2119(1) (Carjacking); 18 U.S.C. §§ 924(c)(1)(A)(ii) (Carrying, Using, and Brandishing a Firearm During and in Relation to a Crime of Violence); 18 U.S.C. §§ 922(g)(1) and 924(a)(2) (Felon in Possession of a Firearm and Ammunition); 18 U.S.C. §§ 922(a)(6) and 924(a)(2) (False Statement to Acquire a Firearm); and 18 U.S.C. § 371 (Conspiracy) have been committed by WILSON, COCHRUN, and unknown persons.

Jurisdiction

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

6. When the Government obtains records pursuant to §2703, or pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2), and (3). Additionally, the Government may obtain an order precluding Google from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize the investigation. 18 U.S.C. § 2705(b).

Probable Cause

7. In August 2020, Lonnie James WILSON was released from prison after serving the first 13 years of his 15-year state sentence for robbery with a firearm. Following his release, WILSON was supervised by the Oklahoma Department of Corrections.

8. On November 13, 2020, WILSON's girlfriend, Nicole Lynn COCHRUN, visited the 2A Shooting Center in Tulsa, Oklahoma, a federally licensed firearms dealer. When she entered the store, a store employee observed that COCHRUN was

with another man. WILSON later indicated in jail calls that he was the man with COCHRUN during the gun sale. COCHRUN then bought a Radical Firearms LLC RF 15 .300 Blackout caliber pistol, bearing serial number 20-014759. To buy the pistol, COCHRUN filled out an ATF Form 4473, on which she stated she would be the actual buyer/transferee of the pistol. Both the employee and her coworkers remembered the purchase well because COCHRUN came back soon after buying the pistol, upset that it was not chambered in .223 or 5.56mmm, and did not appear to know the specifications of the expensive pistol she was buying.

9. About two to three weeks after buying the pistol, COCHRUN bought several rounds of .300 Blackout ammunition, including Remington-Peters .300 AAC Blackout caliber ammunition and Prvi Partizan .300 Blackout caliber ammunition, from Dong's Guns, Ammo, and Reloading in Tulsa, Oklahoma.

10. On December 9, 2020, A.G. and his girlfriend, J.S., were parked in front of J.S.'s house in North Tulsa chatting and drinking coffee inside A.G.'s Chrysler 200 after finishing the night shift at their job. Suddenly, a gray older model Jeep Cherokee pulled up directly next to the Chrysler, the front passenger window of the Jeep parallel to the driver side of A.G.'s car. A.G. and J.S. saw a bright blue light from the front passenger side of the Jeep. Thinking the light might be from a police officer's flashlight, A.G. rolled down his window. He realized that the blue light was coming from a cool blue weapon mounted tactical light affixed to the left side of what appeared to be an assault rifle. Holding the rifle was a man later identified

through the investigation as WILSON. A.G. and J.S. recalled WILSON was wearing a ski mask and a black jacket with a hood pulled tight around his face. WILSON and another accomplice then ordered A.G. and J.S. to get out of the Chrysler.

11. After A.G. and J.S. complied, WILSON's accomplice got out the Jeep Cherokee and pointed a handgun at them. WILSON then trained his rifle on A.G. and J.S. while his accomplice ordered the couple to hand over their cell phones. A.G. and J.S. stated both phones were iPhone 11s. J.S.'s phone had a unique black cell phone cover bearing the cursive words, "Ti Amo," on the back. After taking their cell phones, the accomplice drove off in A.G.'s Chrysler while WILSON drove off in the Jeep. A.G. and J.S. watched as the Jeep followed the Chrysler northbound on Delaware Avenue before going out of sight.

12. Later that morning, I contacted A.G., who informed me that he'd been able to obtain a new phone. He was able to use the "Find my iPhone" feature and obtained a location for his phone that had been taken in the robbery. He sent me the last known location of the phone: 5632 North Elgin Avenue, Tulsa, Oklahoma, at 0915 hrs. on December 9, 2020. Based on my experience, a "Find my iPhone" ping of a cellular handset is accurate within a few feet. This indicates that the phone was at 5632 North Elgin Avenue at the time it was pinged.

13. I learned from another officer that this house was a known 57 Hoover Crips stash house. I reviewed public records for the house, including utilities bills that

listed certified Hoover Crips members as the payors, and social media of known Hoover Crip gang members that featured the house as a hangout location. According to his Oklahoma Department of Correction records, WILSON is a certified 57 Hoover Crips member. The Tulsa Police Department ("TPD") also lists WILSON as a certified 57 Hoover Crips member.

14. After receiving the address, I drove to 5632 North Elgin Avenue. There were no cars in the driveway, however, the front door behind the storm door was standing open, indicating that the house was occupied. I located the victim's stolen Chrysler 200 just north of the house in front of 345 East 57th Place North. I observed that the license plate of the Chrysler had been removed. Based on my training and experience, it is common for suspects to park stolen vehicles nearby, in the neighborhood where they are staying, instead of in front of the house where they are staying. This is done to prevent drawing the attention of law enforcement to the address where the suspects are staying. Investigators later reviewed the vehicle records for the victim's stolen Chrysler and determined that the Chrysler traveled in interstate and/or foreign commerce to reach the state of Oklahoma.

15. On December 10, 2020, the next day, I and other TPD officers served a search warrant at the stash house. During the search, I recovered a black iPhone case with the cursive words, "Ti Amo," from inside a trash can. I confirmed with J.S. that this phone case belonged to her and had been stolen during the carjacking.

16. On December 11, 2020, the next day, TPD officers patrolling the area of 4900 Martin Luther King Jr. Boulevard noticed a silver Pontiac speeding eastbound on 49th Street North. When the officers followed the Pontiac, it Pontiac sped up and made several erratic turns in an apparent attempt to evade officers. When officers eventually stopped the Pontiac, one backseat passenger fled and was later found hiding in a trash can.

17. When officers approached the Pontiac, WILSON, who was seated in the front passenger seat, told them that there was a gun inside the car. Obeying officer's commands, WILSON got out of the Pontiac. Officers then spotted an AR-style pistol resting against the center console next to the front passenger side seat where WILSON had been sitting moments earlier. This pistol was the same Radical Firearms LLC RF 15 .300 Blackout caliber pistol, bearing serial number 20-014759, that COCHRUN purchased on November 13, 2020. Officers observed the pistol was equipped with a "brass catcher" on the ejection port and a cool blue weapon mounted tactical light affixed to the left side of the pistol. The pistol also had a makeshift sling fashioned out of a purse strap. The strap was attached to the pistol with black zip ties. Officers also found the pistol was loaded with 22 rounds of .300 Blackout caliber ammunition, specifically 19 rounds of Remington-Peters .300 AAC Blackout caliber ammunition and Prvi Partizan .300 Blackout caliber ammunition. These were the same make and caliber of ammunition that COCHRUN purchased after buying the pistol. An ATF agent later examined the firearm and ammunition,

and determined that the firearm and each round of ammunition traveled in interstate and/or foreign commerce to reach the state of Oklahoma.

18. After detaining its occupants, officers searched the Pontiac. During the search, officers located the missing license plate for A.G.'s Chrysler and the purchase agreement paperwork for the Chrysler with A.G.'s information stuffed inside a red/orange "fanny pack" inside the trunk. A.G. later confirmed that the red/orange fanny pack had been in his Chrysler at the time of the carjacking.

19. Officers then located a backpack belonging to WILSON. The backpack contained his wallet, including his Oklahoma ID, hand tools, black zip ties matching those found on the pistol, and a black stocking cap.

20. Officers also retrieved cell phones belonging to WILSON and COCHRUN. WILSON's cell phone was a silver LG cell phone, with IMEI: 354855111935978. I later learned WILSON's phone number associated with the LG phone was (918)-523-0134. I was able to confirm this when I searched the phone number using ZetX, a cell phone investigation service. I learned that (918)-523-0134 is a Metro PCS number, registered to "Fenda" WILSON. "Fenda" is WILSON's nickname. WILSON also refers to himself as "Fenda" in his prerecorded jail message at the Tulsa County jail, where he is currently detained.

21. Following the search, WILSON and the other occupants of the Pontiac were transported to the TPD Detective Division. I and another detective then met with WILSON and the other occupants at the Detective Division. After waiving his

Miranda rights, WILSON told me that he had recently been released from prison after serving a long sentence for robbery, that he knew he should not have been around the pistol, and that the pistol belonged to COCHRUN.

22. During his interview, WILSON denied involvement in the carjacking. WILSON stated the silver Pontiac belonged to his brother, but that it had been in his possession at the time of the robbery, making it unlikely that anyone else had placed the victim's property in the trunk of the vehicle. WILSON further stated that he believed he was "somewhere" asleep at the time of the robbery, stating he had either slept at COCHRUN's house in Broken Arrow or his mother's house. WILSON added that the pistol did not go anywhere without him, cutting off his statement as he realized he was admitting to taking the gun everywhere with him. I was able to confirm both COCHRUN's address and his mother's address during this investigation. I further confirmed that his mother lives in Osage County and therefore outside of Tulsa city limits.

23. I subsequently authored a search warrant for cell phone location data on WILSON's number at the time of the carjacking. That search warrant produced no GPS location data or tower data at the exact time the carjacking occurred, indicating that WILSON's phone may have been turned off during that period. However, the ping data reflected that Wilson traveled to the area of the carjacking in the early morning hours of December 9, 2020. He then traveled to the area of 5632 North

Elgin Avenue, before his signal becomes lost. Based on my training and experience, such gaps in ping data can be caused by a phone user turning off their device.

24. Approximately an hour after the carjacking, WILSON's phone began pinging off towers again. At that time, WILSON's phone utilized a cell tower located at 3844 North Martin Luther King Avenue, in Tulsa, Oklahoma. Approximately one hour later, his phone utilized a tower at 508 East 56th Street North, less than a quarter mile from where I located the victim's vehicle and in the immediate vicinity of 5632 North Elgin Avenue. WILSON then received a rapid succession of incoming calls and text messages from the phone number (785) 317-7764, every few minutes. I recognized this phone number as the one associated with COCHRUN's phone seized during the December 11, 2020 traffic stop.

25. Accordingly, the ping data for WILSON's phone contradicts his statement that he was asleep at the time of the robbery either at COCHRUN's house in Broken Arrow or at his mother's house in Osage County. Based on the foregoing, it is likely that WILSON cased the area of the carjacking prior to the carjacking, traveled to the area of 5600 North Elgin Avenue to pick up an accomplice or obtain other items or a vehicle to use in the carjacking, turned off his phone to evade detection during the carjacking, turned his phone back on following the carjacking, and then returned to the area of 5632 North Elgin Avenue later that morning to deposit the victim's car in the neighborhood and drop off the stolen items at the house.

26. On December 8, 2021, while reviewing my interview of WILSON, I noticed that WILSON stated that he had been working at Resource One in December 2020, up until his arrest. I then contacted an employee with Human Resources for Resource One located at 2900 East Apache Street, Tulsa, Oklahoma. The employee stated that her records did show that WILSON had been employed there in December 2020, but that he had been terminated from his job. She provided the email address that Mr. WILSON used when he applied with Resource One, **fendawilson@gmail.com** ("Subject Account"). This username is consistent with publicly available Facebook accounts for WILSON and the account information for WILSON's phone.

27. On December 15, 2021, I made a request to Google pursuant to 18 U.S.C. § 2703(f), requesting Google to preserve all information associated with the Subject Account.

Background Concerning E-Mail Providers and Google

28. In the Affiant's training, experience, and research, Affiant learned e-mail providers such as Google usually maintain the following records and information with respect to subscriber accounts:

a. *E-mail content.* In general, any e-mail (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the e-mail providers' servers unless and until the subscriber deletes the e-mail. If the subscriber does not delete the e-mail, it

can remain on the provider's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on the provider's servers for a certain period of time.

b. *Address Book.* E-mail providers usually also allow subscribers to maintain the equivalent of an address book, comprising e-mail addresses and other contact information of other e-mail users.

c. *Device Information.* E-mail providers can collect and maintain information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers, Mobile Electronic Identify Numbers, Mobile Equipment Identifiers, Mobile Identification Numbers, Subscriber Identity Modules, Mobile Subscriber Integrated Services Digital Network Number, International Mobile Subscriber Identifiers, or International Mobile Equipment Identities.

d. *Subscriber and billing information.* The e-mail provider can collect and maintain (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate e-mail addresses. The e-mail providers can also maintain records concerning the date on which the account was created, the Internet Protocol address of the user at the time of account creation, the current status of the account (e.g., active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying

subscribers, the e-mail provider can also maintain records of the subscriber's means and source of payment, including a credit card or bank account number

e. *Cookie Data.* E-mail providers can use features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at the e-mail provider using the same computer. One of the ways e-mail providers accomplish this is by using cookies, a string of characters stored on the user's computer or web browser that is recognized by the e-mail provider when a computer visits its website or logs into an account.

f. *Transactional Information.* The e-mail providers typically retain certain transactional information about the use of an account. This information can include records of login (i.e. session) times and durations and the methods used to connect to the account.

g. *Location History.* E-mail providers can also collect data on the location of their users from their electronic devices. E-mail providers use this information for, among other things, location-based advertising, location-based search results, embedding location information in photographs and videos taken by the user (known as geo-tagging), navigation through maps and services and related applications, and features that permit users to locate their mobile electronic devices if they lose them.

h. *Customer correspondence.* E-mail providers can also maintain records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

i. *Preserved and backup records.* E-mail providers can also maintain preserved copies of the foregoing categories of records with respect to an account, for 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. Section 2703(f).

29. In the Affiant's training, experience, and research, Affiant has learned Google also maintains records with respect to other Google services, which it stores in connection with e-mail accounts, which can include, in part, the following:

a. *Google Drive Content.* Google can provide users with a certain amount of free cloud storage, which is currently approximately 15 gigabytes, through a service called Google Drive. Users can purchase a storage plan through Google to store additional content. Users can use their Google Drive to store e-mail, attachments, videos, photographs, documents, and other content "in the cloud," that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

b. *Google Docs.* Google can provide users with the ability to write, edit, and collaborate on various documents with other Google users through a service called Google Docs. Users can use Google Docs to create online documents which can be stored on or saved to the user's Google Drive.

c. *Google Photos.* Google can provide users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to store photographs and videos. Google also retains the metadata-or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata can include what is known as exchangeable image file format (EXIF) data, and can include GPS location information for where a photo or video was taken.

d. *Google Calendar.* Google provides users with an online calendar, in which they can add appoints, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

e. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in "chat" sessions in an instant messaging format with other Google users. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which can permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user's e-mail and chat content.

f. *Location History Data.* Google can maintain recent location data, collected periodically, from mobile devices that are logged into or have used applications or services provided by Google. For example. Google can collect information collected from GPS, or Wi-Fi networks, cell site locations, and mobile networks to estimate a

user's location Google applications and services can also allow for location reporting, which allows Google to periodically store and use a device's most recent location data in connection with a Google account.

g. *Google Payments.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

h. *Chrome Browser and Search History.* Google can store information regarding user Internet browser activity when a Google user is logged into his or her account, which includes logging information about websites viewed by the user, Internet search queries in the Google Internet search engine available at http://www.google.com, and also maintains lists of bookmarks maintained by the user so that he or she can quickly access frequently viewed websites.

Evidence of Criminal Conduct under Investigation Stored in Connection with E-Mail Accounts

30. As explained herein, information stored in connection with an e-mail account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In affiants training and experience, the information stored in connection with an email

account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the e-mail provider can show how and when the account was accessed or used. For example, as described above, e-mail providers typically log the Internet Protocol addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

31. Based on my training and experience, Google collects and retains location data from Android enabled mobile devices like WILSON's LG phone. The company uses this information for location-based advertising and location- based search results. Per Google, this information is derived from Global Position System (GPS) data, cell site/cell tower information, and Wi-Fi access points. While the specific parameters of when this data is collected are not entirely clear, it appears that Google collects this data whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text message, internet access, or email access. Your affiant believes that this data will show the movements of the suspect's mobile device and assist investigators with establishing patterns of movement, identifying residences, work locations, and other areas that may contain further evidence relevant to the criminal investigation of WILSON, COCHRUN, and unknown co-conspirators.

Review of Information Obtained Pursuant to the Warrant

32. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to Google LLC, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the Government in this

investigation, and outside technical experts under government control) will retain the records and review them for evidence and instrumentalities of the Subject Offenses as specified in Attachment B to the proposed warrant.

33. In conducting this review, law enforcement personnel may use various methods to locate evidence and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all information within the Subject Account(s). This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, affiant knows that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with e-mails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications, and consequently there are often many

communications in an account that are relevant to an investigation but do not contain any keywords that an agent is likely searching for.

Conclusion

34. Based on the forgoing, I request that the Court issue the proposed search warrant. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

BRYANT WARD
TULSA POLICE DEPARTMENT

Subscribed and sworn to ~~before~~ by telephone me on December 17, 2021, 2021

HON. SUSAN E. HUNTSMAN
UNITED STATES MAGISTRATE JUDGE

Attachment A

Property to Be Searched

This warrant applies to information associated with **fendawilson@gmail.com** ("Subject Account"), from November 13, 2020 to December 11, 2020, that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

Attachment B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on December 15, 2021, Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from November 13, 2020 to December 11, 2020, unless otherwise indicated:

a. *E-mail Content.* All e-mails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination address associated with each email, the date and time at which each e-mail was sent or received, and the size and length of each e-mail), limited to items sent, received, or created between November 13, 2020 to December 11, 2020.

b. *Address Book Information.* All address book, contact list, or similar information associated with the Subject Account.

c. *Google services Information.* The files and contents with the account related to Google Services, including Google Drive, Google, Docs, Google Photos,

Google Calendar, Google Chats, Google, Hangouts, Web Search and History, and Google Payments.

d. *Subscriber and Payment Information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

e. *Search and web history records.* All records relating to web and application activity history (including search terms), device information history, and location history.

f. *Device Information.* Any information identifying the device or devices used to access the Subject Account, including a device serial number, a GUID or Global Unique Identifier, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identify Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI") and any other information regarding the types of devices used to access the Subject Account.

g. *Information Regarding Linked Accounts including Linked By Cookie.* Any information identifying accounts that are associated or connected to the Subject Account, including specifically by cookie, Google Account Id, Android ID, or other

account or device identifier (the "Linked Accounts") to include names, addresses, local and long-distance telephone connection records, records of session times and durations, length of service, telephone or instrument numbers, other subscriber numbers or identities, means and source of payment for service and billing records.

h. *Location Data*. All location data associated with the Subject Account, including GPS data, cell site/cell tower triangulation/trilateralization, and wi-fi location, including GPs coordinates and dates and times of all location recordings.

i. *Transactional Records*. All transactional records associated with the Subject Account, including IP logs or other records of session times and durations.

j. *Customer Correspondence*. All correspondence with the subscribers or others associated with the Subject Account including complaints, inquiries, or other contacts with support services and records of action.

k. *Preserved or backed up records*. Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 United States Code, Section 2703(f) or otherwise.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2119(1) (Carjacking); 18 U.S.C. §§ 924(c)(1)(A)(ii) (Carrying, Using, and Brandishing a Firearm During and in Relation to a Crime of Violence); 18 U.S.C. §§ 922(g)(1) and 924(a)(2) (Felon in Possession of a Firearm and Ammunition); 18 U.S.C. §§ 922(a)(6) and 924(a)(2) (False Statement to Acquire a Firearm); and 18 U.S.C. § 371 (Conspiracy) involving

Lonnie James WILSON, Nichole Lynn COCHRUN, and unknown persons from November 13, 2020 to December 11, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. E-mail or other communications between Lonnie James WILSON and co-conspirators, including Nichole Lynn COCHRUN, concerning robberies, carjacking, or the possession, sale, or use of firearms.

b. Information identifying the user or the location of the user of the Subject Account, and the individuals involved, including photographs or videos depicting that the user, the Subject Account, trusts, which reveal his or her identity to include information that can be used to ascertain his/ her identity, such as travel information or receipts for online purchases or other communications with social network websites or third party service providers;

c. Communications of the user of the Subject Account with co-conspirators and others about the offenses enumerated herein.

d. Evidence of searches related to the victim, the victim's address, or of searches related to robbery, carjacking, or the possession, sale, or use of firearms.

e. Evidence of travel destinations, directions, or location information related to Subject Account that would confirm or dispute the involvement of the user of Subject Account in the offenses enumerated herein.

f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s) from November 13, 2020 to December 11, 2020.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Certificate of Authenticity of Domestic Records Pursuant to Federal Rules of Evidence 902(11) and 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google LLC. The attached records consist of _____. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google LLC, and they were made by Google LLC as a regular practice; and

b. such records were generated by Google LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature